known only to the user and to the electronic system, which checks the identifier against data in a database to authenticate the user's identity.

Public/private key (asymmetric) cryptography is a method of creating a unique mark, known as a digital signature, on an electronic document or file. This method involves the use of two computer-generated, mathematically-linked keys: a private signing key that is kept private and a public validation key that is available to the public.

RFEHB means the Retired Federal Employees Health Benefits Program established under Pub. L. 86–724, 74 Stat. 849, 851–52 (September 8, 1960), as amended.

Shared service centers are processing centers delivering a broad array of administrative services to multiple agencies.

Shared symmetric key cryptography means a method of authentication in which a single key is used to sign and verify an electronic document. The single key (also known as a "private key") is known only by the user and the recipient or recipients of the electronic document.

Smart card means a plastic card, typically the size of a credit card, containing an embedded integrated circuit or "chip" that can generate, store, or process data. A smart card can be used to facilitate various authentication technologies that may be embedded on the same card.

§ 850.104 Implementing directives.

The Director must prescribe, in the form he or she deems appropriate, such detailed procedures as the Director determines to be necessary to carry out the purpose of this part.

§ 850.105 Agency responsibility.

Agencies employing individuals whose retirement records or processing are affected by this part are responsible for counseling those individuals regarding their rights and benefits under CSRS, FERS, FEGLI, FEHB, or RFEHB.

§ 850.106 Electronic signatures.

(a) Subject to any provisions prescribed by the Director under § 850.104—

(1) An electronic communication may be deemed to satisfy any statutory or regulatory requirement under CSRS, FERS, FEGLI, FEHB or RFEHB for a written election, notice, application, consent, request, or specific form format;

(2) An electronic signature of an electronic communication may be deemed to satisfy any statutory or regulatory requirement under CSRS, FERS, FEGLI, FEHB or RFEHB that an individual submit a signed writing to OPM;

(3) An electronic signature of a witness to an electronic signature may be deemed to satisfy any statutory or regulatory requirement under CSRS, FERS, FEGLI, FEHB or RFEHB for a signature to be witnessed; and

(4) Any statutory or regulatory requirement under CSRS, FERS, FEGLI, FEHB or RFEHB that a signature be notarized may be satisfied if the electronic signature of the person authorized to sign is attached to or logically associated with all other information and records required to be included by the applicable statute or regulation.

(b) For purposes of this section, an electronic signature is a method of signing an electronic communication, including an application, claim, or notice, designation of beneficiary, or assignment that—

(1) Identifies and authenticates a particular person as the source of the electronic communication; and

(2) Indicates such person's approval of the information contained in the electronic communication.

(c) The Director will issue directives under § 850.104 that identify the acceptable methods of effecting electronic signatures for particular purposes under this part. Acceptable methods of creating an electronic signature may include—

(1) Non-cryptographic methods, including—

(i) Personal Identification Number (PIN) or password;

(ii) Smart card;

(iii) Digitized signature; or

(iv) Biometrics, such as fingerprints, retinal patterns, and voice recognition;

(2) Cryptographic control methods, including—

(i) Shared symmetric key cryptography;